

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

AMELIA INGRAO and ELISABETH
PACANA, individually and on behalf of all
others similarly situated,

Plaintiff,

v.

ADDSHOPPERS, INC., NUTRISYSTEM,
INC., VIVINT, INC.,

Defendants.

Case No. 2:24-cv-1022

CONSOLIDATED MEMORANDUM IN OPPOSITION TO MOTIONS TO DISMISS

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	FACTUAL BACKGROUND	2
III.	LEGAL ARGUMENT	5
A.	Legal Standard	5
B.	The Court Can Exercise Personal Jurisdiction Over Defendants.	6
C.	Plaintiffs Have Standing To Pursue Their claims In Federal Court.....	9
D.	Plaintiffs plead plausible California and Pennsylvania wiretapping claims against Defendants for their participation in a mass surveillance program.	11
1.	Vivint wiretapped Plaintiff Pacana before she could ostensibly “consent.”	16
2.	Plaintiff Pacana was not on actual or constructive notice of Vivint’s privacy policy... ..	16
E.	Plaintiffs Adequately Plead A Violation Of The CDAFA.....	17
F.	The Court Should Not Strike The Class Allegations.	19
G.	The First-Filed Rule Does Not Apply Here.	20
IV.	CONCLUSION.....	23

TABLE OF AUTHORITIES**Cases**

<i>Akerman v. Oryx Communications, Inc.,</i> 609 F. Supp. 363 (S.D. N.Y. 1984)	19
<i>Ashcroft v. Iqbal,</i> 556 U.S. 662 (2009).....	6
<i>Augustine v. Lenovo (U.S.), Inc.,</i> 2023 WL 4938050 (S.D. Cal. Aug. 2, 2023).....	15
<i>Bane v. Netlink, Inc.,</i> 925 F.2d 637 (3d Cir. 1991)	6
<i>Braun v. Philadelphia Inquirer, LLC,</i> 2023 WL 7544160 (E.D. Pa. Nov. 13, 2023).....	9, 12, 17
<i>Briskin v. Shopify, Inc.,</i> 87 F.4th 404 (9th Cir. 2023).....	8
<i>Briskin v. Shopify, Inc.,</i> 101 F.4th 706 (9th Cir. 2024).....	8
<i>Brown v. Google LLC,</i> 685 F. Supp. 3d 909 (N.D. Cal. 2023)	18
<i>Constitution Party of Pa. v. Aichele,</i> 757 F.3d 347 (3d Cir. 2014)	5
<i>Cook v. GameStop, Inc.,</i> 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023)	10, 12, 13
<i>COR Sec. Holdings Inc. v. Banc of California, N.A.,</i> 2018 WL 4860032 (C.D. Cal. Feb. 12, 2018).....	18
<i>Danziger & DeLlano, LLP v. Morgan Verkamp LLC,</i> 948 F.3d 124 (3d Cir. 2020)	6
<i>Doe v. FullStory, Inc.,</i> 2024 WL 188101 (N.D. Cal. Jan. 17, 2024)	8
<i>E.E.O.C. v. Univ. of Pennsylvania,</i> 850 F.2d 969 (3d Cir. 1988)	20, 21
<i>Farst v. AutoZone, Inc.,</i> 2023 WL 7179807 (M.D. Pa. Nov. 1, 2023).....	10, 13

<i>Gibbs v. Haynes Investments, LLC,</i> 368 F. Supp. 3d 901 (E.D. Va. 2019)	22
<i>Grandalski v. Quest Diagnostics Inc.,</i> 767 F.3d 175 (3d Cir. 2014)	19
<i>Greenley v. Kochava, Inc.,</i> 2023 WL 4833466 (S.D. Cal. July 27, 2023).....	18
<i>Grider v. Keystone Health Plan Cent., Inc.,</i> 500 F.3d 322 (3d Cir. 2007).....	21
<i>Hasson v. FullStory, Inc.,</i> 2023 WL 4745961 (W.D. Pa. July 25, 2023).....	7
<i>Hazel v. Prudential Fin., Inc.,</i> 2023 WL 3933073 (N.D. Cal. June 9, 2023)	14
<i>IMO Indust., Inc. v. Kierkert AG,</i> 155 F.3d 254 (3d Cir. 1998)	7
<i>In re Google Inc. Cookie Placement Consumer Priv. Litig.</i> 806 F.3d 125 (3d. Cir. 2015)	9, 12, 15
<i>In re Thalomid and Revlimid,</i> 2015 WL 9589217 (D.N.J. Oct. 29, 2015).....	19
<i>In re Yahoo Mail Litig.,</i> 308 F.R.D. 577 (N.D. Cal. 2015)	19
<i>James v. Walt Disney Co.,</i> 2023 WL 7392285 (N.D. Cal. Nov. 8, 2023).....	12
<i>Javier v. Assurance IQ, LLC,</i> 2022 WL 1744107 (9th Cir. May 31, 2022).....	11
<i>La Mar v. H & B Novelty & Loan Co.,</i> 489 F.2d 461 (9th Cir. 1973).....	19
<i>Landsman & Funk PC v. Skinder-Strauss Assocs.,</i> 640 F.3d 72 (3d Cir. 2011)	19
<i>MacLean v. Wipro Ltd.,</i> 2020 WL 7090746 (D.N.J. Dec. 4, 2020)	20, 21
<i>Mallory v. Norfolk S. Ry. Co.,</i> 143 S. Ct. 2028 (2023).....	6

<i>Martin v. Medicredit, Inc.,</i> 2016 WL 6696068 (E.D. Mo. Nov. 15, 2016)	21
<i>McClung v. AddShopper, Inc.,</i> 2024 WL 189006 (N.D. Cal. Jan. 17, 2024)	passim
<i>MLI RX, LLC v. GlaxoSmithKline LLC,</i> 2023 WL 3739064 (E.D. Pa. May 30, 2023)	22
<i>Motley v. ContextLogic, Inc.,</i> 2018 WL 5906079 (N.D. Cal. Nov. 9, 2018).....	16
<i>NovelPoster v. Javitch Canfield Grp.,</i> 140 F. Supp. 3d 938 (N.D. Cal. 2014)	18
<i>Oliver v. Noom,</i> 2023 WL 8600576 (W.D. Pa. Aug. 22, 2023).....	12, 16, 17
<i>Popa v. Harriet Carter Gifts, Inc.,</i> 52 F.4th 121 (3d Cir. 2022)	13
<i>Price v. Carnival Corp.,</i> 2024 WL 221437 (S.D. Cal. Jan. 19, 2024).....	15
<i>Revitch v. New Moosejaw, LLC,</i> 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019).....	14
<i>Ricoh Co. v. Honeywell, Inc.,</i> 817 F. Supp. 473 (D.N.J. 1993)	21
<i>Rodriguez v. Google LLC,</i> 2021 WL 2026726 (N.D. Cal. May 21, 2021)	18
<i>Russo v. Microsoft Corp.,</i> 2021 WL 2688850 (N.D. Cal. June 30, 2021)	13
<i>S.D. v. Hytto Ltd.,</i> 2019 WL 8333519 (N.D. Cal. May 15, 2019)	7
<i>Sacco v. Mouseflow, Inc.,</i> 2022 WL 4663361 (E.D. Cal. Sept. 30, 2022).....	7
<i>Saleh v. Nike, Inc.,</i> 562 F.Supp.3d 503 (C.D. Cal. 2021).....	7
<i>Smith v. S.E.C.,</i> 129 F.3d 356 (6th Cir. 1997)	21

<i>Spokeo, Inc. v. Robins,</i> 578 U.S. 330 (2016).....	9
<i>Valenzuela v. Nationwide Mut. Ins.,</i> 2023 WL 5266033 (C.D. Cal. Aug. 14, 2023)	14
<i>Weske v. Samsung Elecs. Am., Inc.,</i> 934 F. Supp. 2d 698 (D.N.J. 2013)	19
<i>Worthington v. Bayer Healthcare, LLC,</i> 2012 WL 1079716 (D.N.J. Mar. 30, 2012)	21
<u>Statutes</u>	
42 Pa.C.S.A. § 5301(a)(2)(i) & (a)(3)(i)	6
18 Pa.C.S.A. § 5725(a)	11
Cal. Penal Code § 502(c)(1), (6)-(7)	18

I. INTRODUCTION

“AddShoppers” and “SafeOpt.” These names are unfamiliar to most consumers until they receive an “abandoned item” email from a retailer to whom they provided no personal information. But behind the scenes, with retailers’ help, AddShoppers has built a mass surveillance enterprise called “SafeOpt.” Through SafeOpt, AddShoppers runs what it calls a “Data Co-Op” that collects information about individuals from multiple sources so it can send direct advertisements on behalf of Co-Op members—taking a cut of every sale. To do this, AddShoppers installs malicious third-party tracking cookies on users’ browsers and then tracks their web activity as they browse the internet, alerting it the moment the user lands on the website of one of its retail partners. Those retail partners collectively sell every imaginable good: men’s health products, women’s hygiene products, coffee, guns, medical supplies, and more.

And because retail partners like Nutrisystem and Vivint have installed the SafeOpt tracking software on their websites, AddShoppers knows exactly what products a potential customer viewed. This information is then added to AddShoppers’ growing dossier on the unconsenting target. Worse still, AddShoppers is purportedly granted a “license” by its retail partners to use the target’s personal information to send direct advertisements on behalf of “each Data Co-Op member’s audience” and to “exploit” for any other purpose it deems fit. Unsurprisingly, very few individuals voluntarily opt into this program. Instead, they are unwittingly captured in it when they make a purchase or create an account on a website that—unbeknownst to them—has agreed to participate in the Co-Op.

For good reason, AddShoppers’ “track and conquer” program has been universally condemned by the public. Hundreds of people have complained online about receiving targeted emails from retailers “via SafeOpt” who they never provided with their personal information.

“*Creepy*”, “*sleazy*”, “*disgusting advertising*”, “*unethical*”, and an “*invasion of privacy*” are just a few snippets of the public commentary condemning this unconsented and ultra-invasive marketing practice. The arrangement also violates California and Pennsylvania law in multiple respects.

II. FACTUAL BACKGROUND

“AddShoppers runs a marketing enterprise that illicitly tracks persons across the internet, collects their personal information without consent, and then uses that information to send direct solicitations.” Dkt. No. 1 (Compl.) ¶ 2. It calls this “‘marketing’ program ‘SafeOpt.’” *Id.* ¶ 3. Most people are unwittingly brought into SafeOpt “when they create an account and make a purchase on a website that—unbeknownst to them—is part of the AddShoppers’ Data Co-Op.” *Id.* “AddShoppers surreptitiously collects and pools the sensitive personal information provided by individuals to online retailers in confidence, creates dossiers on those individuals, and then tracks them across the internet to monitor their web browsing for its own financial benefit.” *Id.* ¶ 29.

AddShoppers does business throughout Pennsylvania. *Id.* ¶ 13. Indeed, it partners with many Pennsylvania retailers including Nutrisystem. *Id.* ¶¶ 14. “And it sends thousands (if not millions) of targeted emails to Pennsylvania.” *Id.*

AddShoppers has amassed a network with over two thousand large brands and publishers. *Id.* ¶ 24. These companies sell almost anything imaginable including “highly personal products.” *Id.* ¶ 46. For example, people have received emails imploring them “to return to purchase a breast pump” or products “from a colon cleansing company.” *Id.*

To partner with the company, AddShoppers requires participation in a “Data Co-op” which permits SafeOpt to “leverage[] a shared pool of user data collected by SafeOpt technology” by granting “SafeOpt with a limited, transferable license to their User Data for the purpose of providing identity resolution and direct messaging services for each Data Co-op member’s

audience.” *Id.* ¶ 27. AddShoppers’ terms also permit it to collect all “Client Data” derived from its partner companies, including their customers’ User Data, and states that “SafeOpt may exploit Client Data for any lawful purpose without any duty of accounting or compensation to you.” *Id.* ¶ 28.

AddShoppers’ model relies on using “malicious, third-party tracking cookies.” *Id.* ¶ 33. Retailers place this code on their website after partnering with AddShoppers—which tracks and sends information to AddShoppers about the user’s browsing activity on a real-time basis. *Id.* ¶¶ 36, 49. So “[w]hen an internet user creates an account or makes a purchase with the business, a third-party tracking cookie is created that includes a unique value AddShoppers associates with that user.” *Id.* ¶ 36. This cookie remains “hidden on the user’s browser and automatically sends information to AddShoppers’ SafeOpt domain ‘shop.pe.’ AddShoppers then associates that unique value with the personal information the user provided to the company, which typically includes, at a minimum, full name, address, payment card information, and email address.” *Id.*

Afterward, every time a “user lands on another website in the SafeOpt network, the cookie values ‘sync’ and AddShoppers tracks the user’s activity on the website, including the user’s detailed referrer Uniform Resource Locator (‘URL’).” *Id.* ¶ 37. As a result, AddShoppers “can directly advertise to the user even where the user leaves a website without affirmatively providing any personal information.” *Id.* Typically, it “solicits in the form of a direct email from the retailer ‘via SafeOpt’ imploring a user to return to the website to purchase a product they were looking at, even though the individual never gave their email address to the retailer or authorized such communications.” *Id.* ¶ 41.

Plaintiffs Amelia Ingrao and Elisabeth Pacana are two such recipients—each received an email “via SafeOpt” from a retailer they had never provided any personal information. *Id.* ¶¶ 55,

61. Although neither Plaintiff agreed to the retailers' privacy policy nor provided any personal information, they both were tracked by AddShoppers. *Id.* ¶¶ 60, 68.

Of course, Plaintiffs were shocked to receive their personal browsing history from a company they never provided with their email address or any other personal information. *Id.* ¶¶ 55-68. Plaintiffs are not alone. The Complaint includes dozens of examples of consumers complaining about receiving unsolicited direct communications from a company they did not know was tracking their web browsing:



Luke Hutchison 
@LH

...

New level of creepy overreach: I just clicked on an ad, read the information on the site, and decided not to buy. I did not enter any information into the site. However they somehow disambiguated my identity, and pushed an email to my email address while I was viewing the site.



mia. 
@miamarshall

...

how tf is SafeOpt legal? after visiting a website, not opting into anything, and not entering any info, I was sent a marketing email for that site via SafeOpt. companies should NOT be using this.

See, e.g., Compl. ¶¶ 43-49.

AddShoppers' Better Business Bureau webpage is also flooded with complaints. One user

noted that “I received a marketing re-targeting email from a company I never gave my email to and saw it was connected to ‘SafeOpt’ (another purposefully misleading name to include the word ‘safe’). I should have control over who has my email. It should not be possible to opt into SafeOpt’s ENTIRE NETWORK OF ADVERTISERS just by opting in on ONE of them. Brands should be ashamed to use this service, it is bad for my personal data and it is bad for data security.” *Id.* ¶ 44. Even after users try to opt out, they are not actually removed from the SafeOpt network and continue to receive marketing emails from AddShoppers. *Id.* ¶ 48-49.

“Plaintiffs each had their [personally identifiable information] PII collected by AddShoppers and their online internet browsing monitored and tracked by AddShoppers without their consent.” *Id.* ¶ 69. And “[t]heir information has independent value, which is recognized by AddShoppers and members of the Data Co-Op who agree to collect and trade it for their personal gain. Plaintiffs and class members are harmed every time their PII is used or shared in a manner to which they did not consent, particularly when it is used to solicit them for marketing and advertising purposes.” *Id.* Accordingly, Plaintiffs bring three counts for violations of: (1) Pennsylvania’s Wiretapping and Electronic Surveillance Control Act (Pennsylvania Wiretap Act) (2) the California Invasion of Privacy Act (CIPA); and (3) the California Comprehensive Computer Data Access and Fraud Act (CDAFA).

III. LEGAL ARGUMENT

A. Legal Standard

Defendants move to dismiss under both Fed. R. Civ. P. 12(b)(1) and 12(b)(6). In reviewing a facial attack under Rule 12(b)(1), the Court “must only consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff.” *Constitution Party of Pa. v. Aichele*, 757 F.3d 347, 358 (3d Cir. 2014) (citation omitted). And under

Rule 12(b)(6), a complaint simply must contain “sufficient factual matter, accepted as true, to state a claim to relief that is *plausible* on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

B. The Court Can Exercise Personal Jurisdiction Over Defendants.

a. The Court has general jurisdiction over Vivint.

Under Section 5301(a) of the Pennsylvania Judicial Code, corporations and “similar entities” submit to “general personal jurisdiction” by “qualif[ying] as a foreign entity under the laws of this Commonwealth.” 42 Pa.C.S.A. § 5301(a)(2)(i) & (a)(3)(i). Thus, foreign business entities that register to do business in Pennsylvania are deemed to have consented to the general personal jurisdiction of Pennsylvania courts. *See Bane v. Netlink, Inc.*, 925 F.2d 637, 640-41 (3d Cir. 1991). Because Vivint is registered to business in Pennsylvania, it has already consented to general personal jurisdiction. Compl. ¶ 15. Its arguments to the contrary ignore the Supreme Court’s decision in *Mallory v. Norfolk S. Ry. Co.*, 143 S. Ct. 2028 (2023). There, the Court upheld Pennsylvania’s consent-by-registration statute against a constitutional challenge. *Id.* at 2032.

b. The Court can exercise specific jurisdiction over AddShoppers.

The Court should apply a three-part test to decide whether the court may exercise specific jurisdiction over AddShoppers. Under that test: (1) AddShoppers must have purposefully directed its activities at Pennsylvania; (2) that the claims “arise out of or relate to” those activities; and (3) that exercising personal jurisdiction will not “offend traditional notions of fair play and substantial justice.” *Danziger & DeLlano, LLP v. Morgan Verkamp LLC*, 948 F.3d 124, 129-30 (3d Cir. 2020). AddShoppers’ conduct satisfies this test. AddShoppers limits its challenge to whether it purposefully directed its activities at the Commonwealth.

1. AddShoppers purposefully directs conduct in this forum.

To purposefully direct conduct at a forum, AddShoppers must have (1) committed an intentional tort, (2) with its allegedly tortious conduct “expressly aimed” at Pennsylvania, and (3)

plaintiff felt the brunt of the harm in Pennsylvania. *IMO Indust., Inc. v. Kierkert AG*, 155 F.3d 254, 259-60 (3d Cir. 1998).

i. AddShoppers committed an intentional tort by wiretapping Plaintiffs.

AddShoppers “easily” satisfies the intentional tort requirement by installing a wiretap on a retailer’s website to purposefully intercept electronic communications. *S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *4 (N.D. Cal. May 15, 2019); *see also Saleh v. Nike, Inc.*, 562 F.Supp.3d 503, 512-13 (C.D. Cal. 2021) (wiretapping satisfies the intentional act requirement). AddShoppers can only dispute this element based on a case evaluating a complaint “riddled with factual irregularities.” *Sacco v. Mouseflow, Inc.*, 2022 WL 4663361, at *4 (E.D. Cal. Sept. 30, 2022). Those irregularities prevented “any finding that Defendant engaged in actual interception or transmissions of communications, data, or information from Plaintiff or any California resident.” *Id.* Here, Plaintiffs describe precisely how AddShoppers wiretapped their communications. *See* Compl. ¶¶ 25-42 (“SafeOpt: The Wiretapper”).

ii. AddShoppers expressly aimed conduct at Pennsylvania.

AddShoppers expressly aimed its conduct at Pennsylvania. As in *McClung*, AddShoppers “orchestrates a scheme with thousands of retailers to (1) intercept and collect information that consumers share with those retailers; and (2) use that collection of information to send unwanted emails to the devices of those consumers. Many of the retailers are alleged to be [Pennsylvania] companies” including Nutrisystem. *McClung v. AddShopper, Inc.*, 2024 WL 189006, at *1 (N.D. Cal. Jan. 17, 2024); Compl. ¶ 13-14.

Hasson does not suggest these in forum partnerships lack importance. There, the out-of-state defendant partnered with an *out-of-state retailer*. *Hasson v. FullStory, Inc.*, 2023 WL 4745961, at *2 (W.D. Pa. July 25, 2023). Here, “the alleged contacts between AddShoppers and

[Pennsylvania] retailers are for the express purpose of enabling AddShoppers to collect customer data and conduct unsolicited customer outreach. In other words, the alleged agreements with [Pennsylvania] companies directly caused the harm.” *McClung*, 2024 WL 189006, at *1.

Because AddShoppers directly interacted with Pennsylvania residents like Plaintiff Pacana, its reliance on cases involving “session replay” software is misplaced.¹ Unlike AddShoppers’ tracking technologies, session replay is a tool used to record and playback a user’s interactions on a website to help the website owner learn how users use its website without “the ability to manipulate or use the captured, substantive data for its own ends.” *Doe v. FullStory, Inc.*, --- F.Supp.3d ---, 2024 WL 188101, at *12 (N.D. Cal. Jan. 17, 2024). It only returns customer “data in the form of ‘insights and analytics back to [the client].’” *Id.* at *11. By contrast, AddShoppers’ business purpose is to track customers through a vast Data Co-Op that it can commercially benefit from. It benefits from these contacts because “it takes a cut of all sales made ‘via affiliate links in emails, texts, apps, and content.’” Compl. ¶ 41. So unlike session replay software, AddShoppers directly interacted with Plaintiff Pacana by sending her targeted personalized emails.

Still, AddShoppers suggests that the sending of emails is “irrelevant because none of Plaintiffs’ claims against AddShoppers are based on the sending of emails.” Doc. 31-1 at 17 n.8. But the sending of emails is a direct byproduct and exploitation of the tracking. And unlike the usual interactive website, AddShoppers affirmatively contacts people on an individualized basis.

¹ AddShoppers also contends that the Ninth Circuit’s decision in *Briskin* shows the Court lacks personal jurisdiction. Doc. 31-1 at 12 (citing *Briskin v. Shopify, Inc.*, 87 F.4th 404 (9th Cir. 2023)). This argument was expressly rejected by the *McClung* Court. See *McClung*, 2024 WL 189006, at *1 (“This case is distinguishable from the recently issued *Briskin*” decision as “the alleged contracts between AddShoppers and California retailers are for the express purpose of enabling AddShoppers to collect customer data and conduct unsolicited customer outreach. In other words, the alleged agreements with California companies directly caused the harm.”). In any event, the Ninth Circuit has now ordered the “case be reheard en banc” and thus the “opinion is vacated.” *Briskin v. Shopify, Inc.*, 101 F.4th 706 (9th Cir. 2024).

iii. **AddShoppers knew Plaintiff Pacana would feel the brunt of the harm in Pennsylvania.**

AddShoppers knew harm would occur in Pennsylvania because it placed wiretaps on many Pennsylvania businesses' websites. AddShoppers also "knew that a significant number of Pennsylvanians would visit its partner websites because they form a significant portion of both companies' target market. Compl. ¶ 13. It is no surprise that ties AddShoppers created—by tracking and sending emails—would cause people to feel the harm in Pennsylvania. Plaintiff Pacana, a Pennsylvania resident, is one of those people.

C. Plaintiffs Have Standing To Pursue Their claims In Federal Court.

To establish Article III standing, Plaintiffs must show (1) an injury, (2) that results from Defendants' conduct (3) that a court can redress. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). Vivint is the only defendant to directly challenge standing. It argues that Plaintiffs lack any injury in fact. Doc. 26 at 11-15. But as in *McClung*, the "complaint adequately alleges Article III standing against AddShoppers and the two retailer defendants." *McClung*, 2024 WL 189006, at *1.

Vivint minimizes Plaintiff Pacana's privacy injury as a bare statutory violation. Doc. 26 at 12-13. This argument ignores the heart of the allegations. AddShoppers "misappropriates a person's browsing activity across a network of thousands of online retailers and uses it to barrage the person's devices with unwanted email communications (particularly without giving the person a way to put a stop to the communications)." *McClung*, 2024 WL 189006, at *1 (cleaned up); Compl. ¶ 29. Plaintiffs therefore adequately allege "the type of intrusion on privacy and seclusion that can be vindicated in federal courts." *Id.*; *see also In re Google Inc. Cookie Placement Consumer Priv. Litig. (Google Placement Cookie)*, 806 F.3d 125, 153 (3d. Cir. 2015) (finding standing where defendant compiled users' internet search histories, created detailed user profiles, and served individualized ads based on those policies); *Braun v. Philadelphia Inquirer, LLC*, 2023

WL 7544160, at *4 (E.D. Pa. Nov. 13, 2023) (finding Article III standing for a Pennsylvania wiretapping claim based on the Facebook tracking Pixel).

Of course, this “scheme cannot exist without the participation of the retailers, and the retailers were aware that their participation would cause these intrusions.” *McClung*, 2024 WL 189006, at *1. The “ultimate injury” is the “aggregation of information about a consumer’s browsing history across thousands of retail sites and the systematic dissemination of emails from the AddShoppers’ network based upon that information. The knowing participation in this scheme by a retailer is enough to confer standing for a victim of the scheme to sue that retailer in federal court.” *Id.*

Yet Vivint argues two “session replay” cases prove Plaintiff Pacana lacks standing. Doc. 26 at 13-14. Those plaintiffs’ browsing activity, however, was never tied to their personal information. *Cook v. GameStop, Inc.*, --- F.Supp.3d ---, 2023 WL 5529772, at *4 (W.D. Pa. Aug. 28, 2023) (“Nothing could connect her browsing history to *her*.” (emphasis in original)); *Farst v. AutoZone, Inc.*, --- F.Supp.3d ---, 2023 WL 7179807, at *4 (M.D. Pa. Nov. 1, 2023) (plaintiff “merely claims AutoZone observed and recorded his general actions on its website, revealing his shopping preferences regarding company products.”). These types of “cases do not stand for the proposition that a website only causes a privacy injury where it collects the personal information *itself*. The whole idea of AddShoppers’ scheme is to tie browsing activity on one site with personal information disclosed on another site, obviating the need for the retailers to do it themselves.” *McClung*, 2024 WL 189006, at *2 n.1 (emphasis in original). Simply put, Plaintiffs have standing when their “personal information was captured” by “tracking cookies embedded within the plaintiffs’ personal computers and browsers.” *Cook*, 2023 WL 5529772, at *5.

Vivint relaunders the same Article III standing arguments to contend Plaintiff Pacana also has “no injury or harm that would allow her to pursue a claim under the [Pennsylvania Wiretap Act].” Doc. 26 at 18-21. This argument fails for the same reasons given above. And although Vivint suggests that Plaintiff Pacana lacks a privacy interest over the observation of her shopping at one store, she alleges a far more insidious tracking program. That is, “Imagine if every store you visited would take a picture of you and then share and compare it with neighboring stores until they find one that you are a customer of and has your information. If such an agreement was in place, that store would now share who you are with the store that you are not yet a customer of and then add you to their marketing list. This is exactly what ‘AddShoppers’ does.” Compl. ¶ 42.

D. Plaintiffs plead plausible California and Pennsylvania wiretapping claims against Defendants for their participation in a mass surveillance program.

Plaintiffs adequately allege Defendants intercepted the contents of their communications, without consent, in violation of CIPA and the Pennsylvania Wiretap Act. *See McClung*, 2024 WL 189006, at *3 (denying motion to dismiss CIPA claims against AddShoppers and a retailer). CIPA “makes liable anyone who ‘reads, or attempts to read, or to learn the contents’ of a communication ‘without the consent of all parties to the communication.’” *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022). And the Pennsylvania Wiretap Act bars interception of an electronic communication without prior consent. *See* 18 Pa.C.S.A. § 5725(a).

Defendants dispute five aspects of these claims: (1) whether the contents of Plaintiffs’ communications were captured; (2) whether Plaintiffs’ communications were intercepted in Pennsylvania; (3) whether AddShoppers is a party to the communication under CIPA; and (4) whether Plaintiff Pacana consented to the wiretap. None have merit.

c. Defendants captured the contents of Plaintiffs' communications.

Plaintiffs adequately allege Addshoppers intercepted the contents of their communications under both CIPA and the Wiretap Act. They plead “a broad scheme in which the defendants generally acquired and tracked the [their] internet usage.” *Google Cookie Placement*, 806 F.3d at 139. As in *Google Cookie Placement*, “if it operate[s] as alleged,” it must involve “the collection of at least some ‘content’ within the meaning of the Wiretap Act.” *Id.*

Yet Defendants argue AddShoppers’ interception of URLs is always “record information” not covered by the statutes. Doc. 25 at 7-9, 11-12; Doc. 26 at 16-17; Doc. 31-1 at 19-20. But Defendants’ attempts to construct a bright line rule about URLs contradicts clear Third Circuit law. “In the context of privacy litigation, the Third Circuit Appellate Court stated that URLs could be considered dialing, routing, addressing or signaling information in one context, but in another context these same URLs contain substantive content that could be improperly disclosed.” *Braun v. Philadelphia Inquirer, LLC*, 2023 WL 7544160, at *4 (E.D. Pa. Nov. 13, 2023). Indeed, retailer defendants already made the same argument in *McClung* which was rejected as “unsuccessful, and too weak or undeveloped to deserve a response.” *Compare McClung*, 2024 WL 189006, at *3 with *McClung v. AddShopper, Inc.*, Case 3:23-cv-01996-VC, Doc. 51 at 22 (N.D. Cal.) (“McClung Docket”) (California retailers’ motion to dismiss). And courts routinely decide captured URLs are potentially content under both statutes. *See, e.g., James v. Walt Disney Co.*, --- F.Supp.3d ---, 2023 WL 7392285, at *11 (N.D. Cal. Nov. 8, 2023) (allegation defendant intercepted “information about the webpages they viewed and searches” makes it “unlikely that Plaintiffs are simply implicating record information”) (Pennsylvania Wiretap Act and CIPA); *Oliver v. Noom*, 2023 WL 8600576, at *7 (W.D. Pa. Aug. 22, 2023).

Defendants' citations to session replay cases are again misplaced. Doc. 25; Doc. 26 at 17. Plaintiffs' claims are not tethered to being tracked by a single website. *Cook*, 2023 WL 5529772, at *6-9; *Farst*, 2023 WL 7179807, at *1. Nor do they complain about the tracking of mouse clicks of keystrokes. *See Cook*, 2023 WL 5529772, at *8.

d. Plaintiffs' communications were intercepted in Pennsylvania (among other places).

Plaintiffs adequately plead that AddShoppers intercepted their communications in Pennsylvania. Vivint acknowledges one point of interception is the place where Plaintiff Pacana accessed its website. Doc. 26 at 24. And because she is a Pennsylvania resident, the reasonable inference is she accessed the website using a computer in the Commonwealth. The Third Circuit's decision in *Popa* does not suggest these allegations are deficient. Instead, it holds that parties must point to material facts "about where the interception occurred" at the *summary judgment stage*. *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 131-32 (3d Cir. 2022).

Plaintiff Ingrao also adequately pleads that Nutrisystem intercepted her communications in Pennsylvania. Nutrisystem wrongly argues that Plaintiff Ingrao "must show that her communications were intercepted from her browser located [in] Pennsylvania." Doc. 25 at 5. Because Nutrisystem is headquartered in the Commonwealth, a Pennsylvania business installed a wiretap on its Pennsylvania website. Then, while visiting that website, Plaintiff Ingrao's communications were collected. Plaintiff Ingrao therefore does not seek to extend liability to conduct wholly outside of Pennsylvania. In *McClung*, the court rejected those retailer defendants' similar argument that out-of-state plaintiffs' communications were not intercepted in California, describing it as "unsuccessful, and too weak or undeveloped to merit a response." *McClung*, 2024 WL 189006, at *3. Besides, the Court should delay deciding the point of interception until it has the benefit of a full evidentiary record. *See Russo v. Microsoft Corp.*, 2021 WL 2688850, at *7

(N.D. Cal. June 30, 2021) (“the Court finds that the precise points of interception is an issue best tested through discovery and does not dismiss on this ground, notwithstanding allegations that plaintiffs’ communications originated in California and Wyoming.”).

e. AddShoppers was not a party to the communication under CIPA.

Plaintiff Ingrao alleges AddShoppers intercepted the contents of her communications in violation of CIPA. Compl. ¶ 131. And Nutrisystem aided and abetted this violation by installing AddShoppers’ wiretaps on its website. *Id.* ¶ 132. A California federal court recently held these same actions taken by AddShoppers and other retailers stated claims for violations of CIPA. *See McClung*, 2024 WL 189006, at *3. But Nutrisystem now argues that AddShoppers is a direct party to the communication. And so, Nutrisystem contends that it cannot be held liable under the direct party exception to CIPA. Doc. 25 at 13. That is wrong.

Indeed, the direct party exception does not extend to retailers when they install a wiretap that financially benefits the third-party wiretapper. *See Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *3 (N.D. Cal. June 9, 2023) (plaintiff adequately stated a claim against both the website operator and third party wiretapper); *Valenzuela v. Nationwide Mut. Ins.*, 2023 WL 5266033, at *6 (C.D. Cal. Aug. 14, 2023) (“Here, Valenzuela alleged that Nationwide hired Akamai specifically to intercept messages and use them for Nationwide’s financial gain. Further, she alleged that Nationwide facilitated Akamai embedding Akamai’s code into Nationwide’s website. These are plausible allegations that Nationwide ‘aided,’ ‘permitted,’ or ‘caused’ Akamai’s violations, which would lead to Nationwide itself being liable” under CIPA.) (cleaned up); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *2 (N.D. Cal. Oct. 23, 2019) (“Although Moosejaw cannot be liable for eavesdropping on its own communications with Revitch, the complaint adequately alleges that Moosejaw violated section 631 by enabling NaviStone’s wrongdoing.”);

see also Augustine v. Lenovo (U.S.), Inc., 2023 WL 4938050, at *3 (S.D. Cal. Aug. 2, 2023) (denying motion to dismiss a CIPA claim where “Plaintiff alleges in the amended complaint that Quantum played an active role in recording including using the data for its own business purposes.”); *Price v. Carnival Corp.*, --- F.Supp.3d ---, 2024 WL 221437, at *3 (S.D. Cal. Jan. 19, 2024) (“Because generating heatmaps and fingerprinting unique browser profiles extends beyond the function of a tape recorder, the ‘party to the communication’ exception does not prevent [defendant] from being ‘held liable under [] federal and state wiretapping statutes for directing, aiding and/or abetting its Session Replay Provider[, Microsoft,] to integrate Session Replay Code into its website.’”). And here, Plaintiff Ingrao alleges AddShoppers “takes a cut of every purchase made via an unauthorized solicitation.” Compl. ¶ 3.

Nor does *Google Cookie Placement* preclude Nutrisystem’s liability for aiding and abetting a wiretap under CIPA for two reasons. First, the Third Circuit only decided direct liability under CIPA, not aiding and abetting liability. *See Google Cookie Placement*, 806 F.3d at 152. And most (if not all) federal courts applying California law have found aiding and abetting liability under these circumstances. Second, the Third Circuit did not preclude direct liability under CIPA for all third-party tracking cookies. Instead, it held that the direct party exception protected deceitful conduct which induced internet users into a false sense of security and continued to track them. *Id.* at 142-43. Here, by contrast, Plaintiff Ingrao has *no relationship* with AddShoppers. As a result, the capture of browsing history here more closely echoes the usual wiretap.

f. Plaintiffs did not consent to the interception of their communications.

Vivint alone argues Plaintiff Pacana “consented” to the conduct here. Doc. 26 at 21. This argument fails for two reasons: (1) the wiretap occurred before she could ostensibly consent; (2) she did not manifest assent to Vivint’s privacy policies.

1. Vivint wiretapped Plaintiff Pacana before she could ostensibly “consent.”

Plaintiffs allege that companies that join AddShoppers’ Data Co-Op install code on their website that automatically sends user information back to AddShoppers via a third-party tracking cookie hidden in the user’s browser. Compl. ¶ 36-37. If the user lands on the website of another partner in the AddShoppers network, the cookie values “sync” and AddShoppers tracks the user’s activity on the website, including the user’s detailed referrer URL, constituting a wiretap. *Id.*, ¶ 37. Vivint is a member of the AddShoppers Data Co-Op and installed AddShoppers’ code on their websites. So Plaintiff Pacana was wiretapped before she could even ostensibly “consent” to such tracking. *See Oliver*, 2023 WL 8600576, at *8 (“These allegations are sufficient to establish, at this stage, that Plaintiffs did not receive notice of (or consent to) Noom’s policies until after the alleged wiretapping took place.”). This is precisely what the court held in *McClung*: “the complaint alleges that the cookies that AddShoppers installs sync with the user’s device the moment that they access the website—thus, by the time the user even sees the cookie banner, the initial visit has already been tracked and linked to AddShoppers’s dossier of browsing activity and personal information.” *McClung*, 2024 WL 189006, at *3. The same is true here.

2. Plaintiff Pacana was not on actual or constructive notice of Vivint’s privacy policy.

Vivint’s website “contained a ‘browsewrap’ agreement, which ‘do[es] not require users to expressly manifest assent’ before accessing the website.” *Oliver*, 2023 WL 8600576, at *8. Indeed, “[b]rowsewrap agreements are properly viewed with skepticism because they purport to create binding contracts on terms a user is not required to review, and in the absence of any affirmative manifestation of agreement by the user.” *Motley v. ContextLogic, Inc.*, 2018 WL 5906079, at *2 (N.D. Cal. Nov. 9, 2018). “[W]hether the terms and conditions in browsewrap agreements are enforceable, often turn[s] on whether the terms or a hyperlink to the terms are reasonably

conspicuous on the webpage[]’ such that a reasonably prudent user would have actual or constructive notice of the relevant conditions.” *Oliver*, 2023 WL 8600576, at *9. Here, Vivint attaches as exhibits printouts of its “Legal Terms and Conditions” and “Privacy Policy” but provides no explanation of how those terms were purportedly presented to Plaintiff Pacana in a manner supporting that she had actual or constructive notice of the relevant conditions. Nor did Plaintiff Pacana consent to such terms. *See* Compl., ¶ 68. Time and again courts have refused to find consent under these circumstances, particularly at the pleading stage. *See Oliver*, 2023 WL 8600576, at *9 (refusing to find consent from browsewrap terms on a motion to dismiss); *Braun v. Philadelphia Inquirer, LLC*, 2023 WL 7544160, at *4 (E.D. Pa. Nov. 13, 2023) (“The question about whether Plaintiffs gave consent to disclosure under the Pennsylvania Wiretapping Act would appear to be factual in nature – involving issues of factual dispute and interpretation.”).²

E. Plaintiffs Adequately Plead a Violation of the CDAFA.

Under CDAFA, a person who commits any of the following acts is guilty of a public offense:

- (1) Knowingly accesses and without permission . . . uses any data, computer, computer system, or computer network in order to . . . wrongfully control or obtain money, property, or data.

- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

² In any event, Vivint’s terms and conditions do not mention or even reference AddShoppers, let alone explicitly notify users that those who visit the website but do not provide any information will have their browsing activity tracked and sent to AddShoppers so it can include them in a Data Co-Op involving thousands of other companies while also granting AddShoppers “with a limited, transferable license to their User Data for the purpose of providing identity resolution and direct messaging services for each Data Co-op member’s audience.” Compl., ¶ 27.

Cal. Penal Code § 502(c)(1), (6)-(7).

Defendants contend that CDAFA’s “without permission” element means that “the defendant ‘circumvent[s] technical or code-based barriers in place’ to prevent unauthorized access.” Doc. 25 at 18 (quoting *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950 (N.D. Cal. 2014)). Defendants also argue that Plaintiff Ingrao “fail to plead damages.” Doc. 25 at 19; Doc. 31-1 at 21. Neither argument is correct.

For starters, CDAFA’s “without permission” element “does not require unauthorized access to information, but rather the unauthorized taking and using of information.” *McClung*, 2024 WL 189006, at *4. The Ninth Circuit therefore “rejected the idea that, under CDAFA, technical circumvention [is] necessary.” *Id.* (citation omitted). So “[c]ode hidden in embedded software may plausibly use or take computer data ‘without permission.’” *Greenley v. Kochava, Inc.*, 2023 WL 4833466, at *14 (S.D. Cal. July 27, 2023). The Court should reject Defendants’ attempt to import the Computer Fraud and Abuse Act’s stricter definition.

“Because plaintiffs have alleged [AddShoppers’] knowing access to, and unpermitted taking of, plaintiffs’ [browsing] activity data, they adequately state a claim under the CDAFA.” *Rodriguez v. Google LLC*, 2021 WL 2026726, at *7 (N.D. Cal. May 21, 2021). Like her CIPA claim, Plaintiff Ingrao has adequately pleaded Nutrisystem assisted AddShoppers’ CDAFA violation. *COR Sec. Holdings Inc. v. Banc of California, N.A.*, 2018 WL 4860032, at *7-8 (C.D. Cal. Feb. 12, 2018) (recognizing aiding and abetting liability).

Plaintiffs also adequately plead damages. *Facebook Tracking* “stands for the proposition that plaintiffs can state an economic injury for their misappropriated data.” *Brown v. Google LLC*, 685 F. Supp. 3d 909, 940 (N.D. Cal. 2023). And Plaintiffs allege that AddShoppers’ appropriation of class members’ PII was to its economic and commercial advantage. Given that AddShoppers

claims a “license” over their information, Plaintiffs also allege they are entitled to the value of the unauthorized access to their [personal information] resulting from Defendants’ wrongful conduct, which can be measured using damages theories analogous to the remedies for unauthorized use of intellectual property (*i.e.*, a “reasonable royalty” from an infringer). Compl. ¶ 70.

F. The Court Should Not Strike The Class Allegations.

Nutrisystem asks the Court to prematurely strike Plaintiff Ingrao’s class allegations. Doc. 25 at 20-22. “In most cases, some level of discovery is essential to [the class certification] evaluation.” *Landsman & Funk PC v. Skinder-Strauss Assocs.*, 640 F.3d 72, 93 (3d Cir. 2011) (vacating decision to strike class allegations at the pleading stage); *see also Weske v. Samsung Elecs. Am., Inc.*, 934 F. Supp. 2d 698, 706-07 (D.N.J. 2013) (“Numerous cases . . . have emphatically denied request to strike class allegations at the motion to dismiss stage as procedurally premature.”). Tellingly, Nutrisystem relies almost exclusively on a case denying class certification. Doc. 25 at 21 (citing *In re Yahoo Mail Litig.*, 308 F.R.D. 577 (N.D. Cal. 2015)). And the choice of law issues it raises are better left for the class certification stage. *See Grandalski v. Quest Diagnostics Inc.*, 767 F.3d 175, 180-183 (3d Cir. 2014) (holding that the proper time to consider choice of law issues for a nationwide litigation class was at the class certification stage).

Plaintiff Ingrao can also pursue and represent class members under the laws of states she does not reside.³ But in any event, the Court should not resolve this issue at this stage. *See In re Thalomid and Revlimid*, 2015 WL 9589217, at *19 (D.N.J. Oct. 29, 2015) (holding whether

³ This is true even as to different defendants. *See La Mar v. H & B Novelty & Loan Co.*, 489 F.2d 461, 466 (9th Cir. 1973); *see also Akerman v. Oryx Communications, Inc.*, 609 F. Supp. 363, 375 (S.D. N.Y. 1984), *judgment aff’d and remanded*, 810 F.2d 336, (2d Cir. 1987) (refusing to certify the class because defendants were not sufficiently unified but describing what might be a sufficient juridical link: “Partnership, joint enterprise, control, conspiracy, *and aiding and abetting all may serve as such a link*, since they denote some form of activity or association on the part of the defendants that warrants imposition of joint liability against the group even though the plaintiff may have dealt primarily with a single member.”) (emphasis added).

plaintiffs may pursue certain state law claims is better left for the class certification stage because ‘the issue now [becomes] one of compliance with the provisions of Rule 23[.]’).

G. The First-Filed Rule Does Not Apply Here.

Defendants argue that the Court should stay this case under the first-filed rule because different plaintiffs filed another case against AddShoppers in the Northern District of California alleging privacy violation claims. *See generally* *McClung* Docket. But any similarities are not enough to trigger the first-filed rule including:

- This case has three Pennsylvania statutory causes of actions absent from *McClung*.
- This case is against two companies over which Pennsylvania can exercise general jurisdiction: (1) Nutrisystem because it is headquartered in the state; and (2) Vivint because it is registered to do business in the state.
- This case is brought by a Pennsylvania resident.
- *McClung* has different retailer defendants—Presidio Brands, Inc. and Peet’s Coffee, Inc.—and now only involves California statutory claims.

Although AddShoppers’ unlawful tracking of plaintiffs’ web browsing with malicious tracking cookies is a common thread to both cases, that alone is insufficient for the Court to stay this case. Indeed, this case differs drastically from *McClung* in several key respects as it involves a Pennsylvania plaintiff, Pennsylvania causes of action, and claims against Nutrisystem and Vivint. Plaintiffs also seek to certify a Pennsylvania Class, which is not represented in the *McClung* action. AddShoppers suggest overlapping counsel matters—it does not.

“The ‘first-filed rule’ or ‘first-to-file rule’ permits ‘trial judges to exercise their discretion by enjoining the subsequent prosecution of similar cases . . . in different federal district courts.’” *MacLean v. Wipro Ltd.*, 2020 WL 7090746, at *5 (D.N.J. Dec. 4, 2020) (quoting *E.E.O.C. v. Univ. of Pennsylvania*, 850 F.2d 969, 971 (3d Cir. 1988) *aff’d*, 493 U.S. 182 (1990)). “Therefore, where related suits ‘involving the same parties and subject matter are pending concurrently, the first-filed

suit should have priority absent a showing that the balance of inconvenience favors transfer or unless there are special circumstances which justify giving priority to the second suit.”” *Id.* (quoting *Ricoh Co. v. Honeywell, Inc.*, 817 F. Supp. 473, 487 (D.N.J. 1993)). “In determining the applicability of the first-filed rule, courts in the Third Circuit examine the chronology of the actions in addition to the overlapping subject matter, issues, claims, and parties.” *Worthington v. Bayer Healthcare, LLC*, 2012 WL 1079716, at *3 (D.N.J. Mar. 30, 2012). “[W]ooden application of the rule” is not required. *E.E.O.C. v. U. of Pennsylvania*, 850 F.2d 969, 972 (3d Cir. 1988), *aff’d*, 493 U.S. 182 (1990). “To be considered parallel proceedings [for purposes of the first-filed rule], the one must be materially on all fours with the other. The issues must have such an identity that a determination in one action leaves little or nothing to be determined in the other.” *Grider v. Keystone Health Plan Cent., Inc.*, 500 F.3d 322, 330 (3d Cir. 2007) (quoting *Smith v. S.E.C.*, 129 F.3d 356, 361 (6th Cir. 1997)) (cleaned up).

Here, the cases lack sufficient overlap to warrant application of the first-filed rule. Applying the rule would deprive these different Plaintiffs of the right to pursue their claims under Pennsylvania law against Defendants Nutrisystem and Vivint, all of which are absent from the *McClung* action. In other words, a resolution of the *McClung* action could only resolve some of Plaintiffs’ claims against AddShoppers and therefore would not “leave[] little or nothing to be determined” in this action. *Grider*, 500 F.3d at 330. Rather, Plaintiffs here would still have their Pennsylvania claims against Nutrisystem and Vivint remaining, which will require discovery and briefing just as the *McClung* action required extensive discovery and briefing for the claims against the different party retailers in that case.

For that reason, courts have held that the first-filed rule should not be applied in similar circumstances. *See, e.g., Martin v. Medicredit, Inc.*, 2016 WL 6696068, at *5 (E.D. Mo. Nov. 15,

2016) (first-filed rule not applied “[b]ased upon the presence of different defendants and significant disparities in the definitions of the putative classes”); *Gibbs v. Haynes Investments, LLC*, 368 F. Supp. 3d 901, 917 (E.D. Va. 2019), *aff’d*, 967 F.3d 332 (4th Cir. 2020) (first-filed rule not applied when plaintiff brought different causes of action under different state laws).

The specific facts here are also incompatible with resolution by a single action against a handful of defendants. Though all Plaintiffs were tracked by AddShoppers’ tracking cookies, they were tracked while visiting different and unrelated websites owned by different defendants. Each individual plaintiff’s claims arise out of their visit to a particular website, not the other websites that other plaintiffs visited. It would be unjust to permit the first-filed action, which names as defendants only websites that those plaintiffs visited, to be the only one that can move forward, while other plaintiffs are left with no ability to pursue their largely unrelated claims against different defendants. This is not a situation where plaintiffs strategically chose different but closely related corporate entities to avoid application of the first-filed rule, instead they filed in a court that can properly exercise jurisdiction over Defendants. Each plaintiff’s claims involve the liability of an unrelated, and the only similarity is the use of AddShoppers’ tracking cookies.

Defendants acknowledge these critical differences, *see* Doc. 31-1 at 29 (“The factual allegations of the two complaints mirror each other, other than the names of the plaintiffs, the websites they visited, and differences in the named defendants outside of AddShoppers.”), and yet rely on case law in which the defendants and claims *are identical* across two actions. *See, e.g.*, *MLI RX, LLC v. GlaxoSmithKline LLC*, 2023 WL 3739064, at *4 (E.D. Pa. May 30, 2023) (“Plaintiffs bring the same claims with *identical allegations against the same Defendants . . .*”) (emphasis added). Such cases are inapposite, as the unique circumstances of this case show that each plaintiff’s claims against different websites are not identical. The remainder of Defendants’

case law simply outlines the guiding principles of the first-filed rule, which should not be applied rigidly, and which, as shown by the facts of this case, guide against application of the rule.

The first-filed rule is based on equitable principles, and as such, cannot serve to bar Plaintiffs from continuing an action involving different plaintiffs, different defendants, different claims, and different state laws. Application of the rule would deprive Plaintiffs of the opportunity to pursue and advance their claims under Pennsylvania law against Defendants Nutrisystem and Vivint—which have no connection to the *McClung* action at all—until the *McClung* action is resolved.

IV. CONCLUSION

Plaintiffs respectfully request that the Court should deny Defendants' motions to dismiss in their entirety, but that any dismissal, in whole or in part, should be without prejudice and with leave to amend.

Dated: June 7, 2024

Respectfully submitted,

By: /s/ Charles E. Schaffer

Charles E. Schaffer

Nicholas J. Elia

LEVIN SEDRAN & BERMAN LLP

510 Walnut Street, Suite 500

Philadelphia, PA 19106

Telephone: (215) 592-1500

cschaffer@lfsblaw.com

nelia@lfsblaw.com

Norman E. Siegel (*pro hac vice*)

J. Austin Moore (*pro hac vice*)

Kasey Youngentob (*pro hac vice*)

STUEVE SIEGEL HANSON LLP

460 Nichols Road, Suite 200

Kansas City, Missouri 64112

(816) 714-7100 (tel.)

siegel@stuevesiegel.com

moore@stuevesiegel.com

youngentob@stuevesiegel.com

Attorneys for Plaintiffs and the Class

CERTIFICATE OF SERVICE

I, Charles E. Schaffer, hereby certify that the foregoing Consolidated Memorandum In Opposition To Motions To Dismiss, was served on this 7th day of June 2024 upon all counsel of record, and unrepresented parties via the Court's electronic notification system.

By: /s/ Charles E. Schaffer
Charles E. Schaffer
Nicholas J. Elia
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com